UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/816,791	04/02/2004	Marco Macchetti	02AG50553433	9927

27975 7590 02/28/2008

ALLEN, DYER, DOPPELT, MILBRATH & GILCHRIST P.A.
1401 CITRUS CENTER 255 SOUTH ORANGE AVENUE
P.O. BOX 3791
ORLANDO, FL 32802-3791

EXAMINER	
SAN JUAN, MARTINJERIKO P	
ART UNIT	**PAPER NUMBER**
2132	

NOTIFICATION DATE	DELIVERY MODE
02/28/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

creganoa@addmg.com

Advisory Action Before the Filing of an Appeal Brief	**Application No.** 10/816,791	**Applicant(s)** MACCHETTI ET AL.	
	Examiner MARTIN JERIKO P. SAN JUAN	**Art Unit** 2132	

--The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

THE REPLY FILED 01 February 2008 FAILS TO PLACE THIS APPLICATION IN CONDITION FOR ALLOWANCE.

1. ☒ The reply was filed after a final rejection, but prior to or on the same day as filing a Notice of Appeal. To avoid abandonment of this application, applicant must timely file one of the following replies: (1) an amendment, affidavit, or other evidence, which places the application in condition for allowance; (2) a Notice of Appeal (with appeal fee) in compliance with 37 CFR 41.31; or (3) a Request for Continued Examination (RCE) in compliance with 37 CFR 1.114. The reply must be filed within one of the following time periods:
   a) ☒ The period for reply expires *3* months from the mailing date of the final rejection.
   b) ☐ The period for reply expires on: (1) the mailing date of this Advisory Action, or (2) the date set forth in the final rejection, whichever is later. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of the final rejection.

   Examiner Note: If box 1 is checked, check either box (a) or (b). ONLY CHECK BOX (b) WHEN THE FIRST REPLY WAS FILED WITHIN TWO MONTHS OF THE FINAL REJECTION. See MPEP 706.07(f).

Extensions of time may be obtained under 37 CFR 1.136(a). The date on which the petition under 37 CFR 1.136(a) and the appropriate extension fee have been filed is the date for purposes of determining the period of extension and the corresponding amount of the fee. The appropriate extension fee under 37 CFR 1.17(a) is calculated from: (1) the expiration date of the shortened statutory period for reply originally set in the final Office action; or (2) as set forth in (b) above, if checked. Any reply received by the Office later than three months after the mailing date of the final rejection, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

NOTICE OF APPEAL

2. ☐ The Notice of Appeal was filed on _____. A brief in compliance with 37 CFR 41.37 must be filed within two months of the date of filing the Notice of Appeal (37 CFR 41.37(a)), or any extension thereof (37 CFR 41.37(e)), to avoid dismissal of the appeal. Since a Notice of Appeal has been filed, any reply must be filed within the time period set forth in 37 CFR 41.37(a).

AMENDMENTS

3. ☐ The proposed amendment(s) filed after a final rejection, but prior to the date of filing a brief, will not be entered because
   (a) ☐ They raise new issues that would require further consideration and/or search (see NOTE below);
   (b) ☐ They raise the issue of new matter (see NOTE below);
   (c) ☐ They are not deemed to place the application in better form for appeal by materially reducing or simplifying the issues for appeal; and/or
   (d) ☐ They present additional claims without canceling a corresponding number of finally rejected claims.

   NOTE: _____. (See 37 CFR 1.116 and 41.33(a)).
4. ☐ The amendments are not in compliance with 37 CFR 1.121. See attached Notice of Non-Compliant Amendment (PTOL-324).
5. ☐ Applicant's reply has overcome the following rejection(s): _____.
6. ☐ Newly proposed or amended claim(s) _____ would be allowable if submitted in a separate, timely filed amendment canceling the non-allowable claim(s).
7. ☐ For purposes of appeal, the proposed amendment(s): a) ☐ will not be entered, or b) ☐ will be entered and an explanation of how the new or amended claims would be rejected is provided below or appended.
   The status of the claim(s) is (or will be) as follows:
   Claim(s) allowed: _____.
   Claim(s) objected to: _____.
   Claim(s) rejected: _____.
   Claim(s) withdrawn from consideration: _____.

AFFIDAVIT OR OTHER EVIDENCE

8. ☐ The affidavit or other evidence filed after a final action, but before or on the date of filing a Notice of Appeal will not be entered because applicant failed to provide a showing of good and sufficient reasons why the affidavit or other evidence is necessary and was not earlier presented. See 37 CFR 1.116(e).
9. ☐ The affidavit or other evidence filed after the date of filing a Notice of Appeal, but prior to the date of filing a brief, will not be entered because the affidavit or other evidence failed to overcome all rejections under appeal and/or appellant fails to provide a showing a good and sufficient reasons why it is necessary and was not earlier presented. See 37 CFR 41.33(d)(1).
10. ☐ The affidavit or other evidence is entered. An explanation of the status of the claims after entry is below or attached.

REQUEST FOR RECONSIDERATION/OTHER

11. ☒ The request for reconsideration has been considered but does NOT place the application in condition for allowance because: See Continuation Sheet.
12. ☐ Note the attached Information *Disclosure Statement*(s). (PTO/SB/08) Paper No(s). _____
13. ☐ Other: _____.

/Gilberto Barron Jr./
Supervisory Patent Examiner, Art Unit 2132

Continuation of 11. does NOT place the application in condition for allowance because: Applicant's arguments filed on February 1, 2008 have been fully considered but they are not persuasive.

Applicant respectfully alleges that Coppersmith does not disclose nor even suggest decoding the input byte into a 256 bit string that contains only one active bit. Moreover, Coppersmith et al. fails to teach or suggest generating output bytes corresponding to respective input bytes according to a one-to-one binary function as in the claimed invention. The equation referenced by the Examiner in column 8, line 16, where Ci is defined, used to generate a mixed byte includes more than one active bit.

The Examiner respectfully disagrees. The Examiner cited equations starting in Col 8, Ln 16 as evidence that generating at least one bit string that contains only one active bit is taught by Coppersmith. It is because of this algorithm that S-boxes depicted in Fig 6 will be used [Col 8, Ln 62 thru Col 9, Ln 10]. Based on the equation, a byte (the input byte) coming from the block of data is used in the one-to-one binary function (as depicted in Col 8, Ln 16) to obtain the index of the substitution value. The substituted values are the output bytes of the generated data blocks of "mixed" bytes. Obtaining a substitution value will inherently involve decoding the index, which is a byte in length in the described embodiment, into a 256-bit string that will contain only one active bit. The S-box has 256 entries, when implemented in hardware [Col 3, Ln 46-47], will inherently require a memory of 256 storage cells participating in the algorithm. Thus it follows that an addressing scheme (ie. the index of the S-box) with 8 active bits (or 1 byte) will be used to map each entry. VLSI basic Memory design teaches the use of decoders to decode n bits into 2^n bit string with only one active bit. Decoders are used to decode the n-active address bits into 2^n bit string with only one active bit so as to map a memory storage cell into a corresponding address spatially. The active bit of the 256 bit string of the decoded address is used to select/activate a memory storage cell. The process of using the 256 bit string with the only one active bit to select and retrieve the corresponding substitution value teaches "encoding the 256 bit string for obtaining an output value." Generating the 8 bit index to be decoded and used to retrieve the S-box substitution value is dictated by Col 8, Ln 16 (This is at least for the left-half mixing part of the entire message block. The right-half mixing is the same except for the incorporation of a displacement value. Refer to Col 9, Ln 45-50 for the right-half mixing algorithm equation.) Col 8, Ln 16 teaches the one-to-one binary function, ie. performing the exclusive ORs of the three operands whose result would be the 8-bit index of the S-box substitution value, and then performing the substitution. Col 8, Ln 16 is a binary function because it takes in inputs, "C", the message byte, and "i" index of message byte being processed. The binary function owes its one-to-one property from the S-box substitution.